EXHIBIT B

Regional Enforcement Allied Computer Team **INVESTIGATION REPORT:** **COVER AND PARTY PAGES**	Case Number: 2018-0066		
	Occurred	Date	Time
	ON OR FROM	Oct 15, 2018	12:00:00 AM
Report Type: 502(c)(1) PC Unlawful Computer Access, 487(a) PC Grand Theft, 530.5(a) PC ID Th	TO	Oct 26, 2018	12:00:00 AM
Location of Crime: 605 West 42nd Street 64W, New York, New York 10036	REPORTED	Oct 19, 2018	12:00:00 AM

SUSPECT INFORMATION AND ASSOCIATED CHARGES

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Truglia, Nicholas	[redacted]	21	M	White	6'3"	200

Home Address	City	State	Zip Code
[redacted]	New York	NY	10036

Phone Number/Type	E-mail Address	DL #	PFN	CII #	Social Security #
[redacted]		[redacted]			[redacted]

Applicable Charge	Description of Charge	
502(c)(1) PC	Unlawful Computer Access	
487(a) PC	Grand Theft	
530.5(a) PC	Identity Theft	
664/487(a) PC	Attempted Grand Theft	

INVOLVED PARTY INFORMATION

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Basu, Saswata	[redacted]	48	M	A		

Address	City	State	Zip Code
[redacted]	Cupertino	CA	95014

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]			Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
2	Ross, Robert	[redacted]	55	M	White		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94118

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
3	Anderson, Angel	[redacted]	46	F	W		

Address	City	State	Zip Code
[redacted]	Los Angeles	CA	90046

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]			[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
4	Danielson, Myles Walker	[redacted]	33	M	W		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94109

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
5	Katsnelson, Gabrielle	[redacted]	34	F	W		

Address	City	State	Zip Code
[redacted]	San Francisco	CA	94133

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT: NARRATIVE

SYNOPSIS:

Victim Saswata Basu, a resident of Santa Clara County, had his AT&T cell phone taken over by the suspect who then gained unlawful access to V. Basu's Yahoo email account and attempted to access his Dropbox account. I was also contacted by Victim Ross who lost access to his cell phone, Gmail account and had approximately $1,000,000 stolen from two cryptocurrency exchanges where the suspects transferred USD into Bitcoin and transferred funds into cryptocurrency wallets the suspects controlled. The suspect also attempted to wire transfer approximately $300,000 from Victim Danielson's Fidelity account but was stopped by the victim. The victims listed in this investigation live within the greater San Francisco Bay Area and Southern California.

BACKGROUND DEFENITIONS:

"Cryptocurrency": Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

"SIM card": For some types of mobile communication devices, a Subscriber Identity Module (or "SIM") card is a small card that is inserted into a mobile device (such as a cell phone handset) to enable the mobile device to communicate with its service provider, as it contains network data needed to make a successful connection to the cellular network provider. SIM cards store files that can be used to uniquely identify them, including the ICCID (Integrated Circuit Card Identifier, a 19- or 20-digit serial number for the SIM card that uniquely identifies the card itself) and the IMSI (International Mobile Subscriber Identity, a 14-or 15- digit number that uniquely identifies a subscriber's account with the cellular network provider).

"SIM swap": An account takeover method by which cellular phone service accounts are compromised. In this scheme, the suspect arranges (through bribery of someone with access,

artifice/"social engineering," or other methods) for a cellular service provider to change the SIM card assigned to particular account to a new SIM card under the suspect's control. Once the suspect controls the new SIM card, he/she can impersonate the victim in correspondence with other service providers (such as email providers) by using the victim's cell phone number to request changes to account settings, eventually resetting the password and taking control of the account.

"IMEI": IMEI is short for International Mobile Equipment Identity is a 15 or 17 digit number that is used to uniquely identify certain types of mobile phone devices. Many providers of electronic communication services log the IMEI number used to access their systems.

2-Factor Authentication ("2FA"): A security mechanism that requires two types of credentials for authentication and is designed to provide an additional layer of validation.

INVESTIGATION:

(V) Saswata B.

Saswata B. is a resident of Santa Clara County. He is a previously reported victim of a SIM swap that occurred in May of 2018 that has been investigated by the REACT Task Force. On 10/18/18, he notified Santa Clara Sheriff's Office Sergeant S. Tarazi that he had just been the victim of another SIM swap, where the target was his phone number ending in -3543. During the incident, the suspects unlawfully accessed his Yahoo email but did not steal any currency or cryptocurrency. AT&T provided records which indicated the mobile communication device utilizing the SIM card used to take over the victim's account during this SIM swap was assigned the IMEI 359239069326461.

(V) Robert R.

On 10/27/1818, at approximately 0800 hours, I began receiving text messages (depicted below) on my department issued cell phone from a phone number [redacted] which I did not recognize.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

I called the number and the voice of a panicked male adult identified himself as (V) Robert R. He gave me the following paraphrased statement over the phone and through email communications:

Robert R. is a resident of San Francisco, California. On 10/26/18, at approximately1800 hours, his cell phone, which uses a phone number ending in -6433, started getting notifications from the "Authy" application seen below which the suspect was controlling.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Gemini is a cryptocurrency exchange in which Robert R. had approximately $500,000 USD, and he had approximately $500,000 more was in a similar account with cryptocurrency exchange Coinbase. At approximately the same time he saw the messages above, Robert R. lost cell service, was logged out of and lost access to his Gmail account ([redacted]), and the suspects took over his "Authy" 2-factor authentication application. He realized a theft was in progress as he could not access any accounts (Gmail, Authy, AT&T or cryptocurrency accounts). He immediately went to an Apple Store where representatives helped him call AT&T Customer Support, who told the victim his SIM card had been changed. Apple inserted a new SIM into his cell phone and AT&T activated the new SIM card, which restored his access to his own phone service.

When this occurred, all of Robert R.'s funds stored on Coinbase (approximately $500,000) and Gemini (approximately $500,000) had been held in USD. The suspect used all the funds in USD at both exchanges to purchase bitcoins, then immediately withdrew all of the bitcoins. Robert R. found this out by looking at transactions on his CoinTracking account, which is connected to his Coinbase and Gemini exchange accounts. This information was subsequently verified by obtaining records directly from Coinbase and Gemini via search warrant.

Robert R. told me he did not sleep at all that night and was up trying to get access to his accounts, figuring out how to retrieve his stolen money and finding someone to help him with the theft. Although he had access to his phone, he was still locked out of his Gmail account, Authy security application, and all of his cryptocurrency accounts. The money stolen was his life savings and money earmarked for his daughter's college fund. He told me many times that he was not sure how he was going to live the rest of his life and send his daughter to college without this money.

Search Warrant to AT&T for records pertaining to IMEI 359239069326461

On 10/29/18, the Honorable Linda Clark, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to accounts linked to the IMEI number 359239069326461. In response, AT&T provided REACT investigators with records that showed the mobile device bearing that IMEI number had been used to effect the account takeovers of both of the victims described above, Saswata B. and Robert R., as well as those of other victims. In total, the records indicated that 11 unique phone numbers had been SIM swapped using this device between 10/15/18 and 10/26/18.

I spoke with the following additional victims who were among the victims listed and whose accounts were taken over using the device bearing IMEI 359239069326461:

(V) Myles D.

I met with this victim in person on 11/6/18 at approximately 0800 hours, and he related the following. Myles D. lives in San Francisco, California. On 10/26/18, at approximately 1530 hours, Myles D.'s

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

AT&T cell phone ([redacted] stopped working while he was at an appointment. Approximately an hour later he confirmed with his wife that her phone was also not working. At approximately 1700 hours, he went to an AT&T Store to try and resolve the issue. The AT&T Store employee pulled the SIM card from his phone and compared the SIM card to the SIM card listed in the account and realized the numbers were different. The employee changed the SIM card back to the original SIM card number and Myles D. regained access to his cell phone service. Once he had phone service back, he checked his Gmail account ([redacted] and learned it was disabled by Google. He contacted Google and had his email access restored, and found out that the suspects had accessed his Gmail account for approximately 4 minutes before Google realized the access was unauthorized and Google disabled the account.

At approximately 1800 hours, he returned to his workplace to look into the hack further because he felt using work computers was safer. He looked in his Gmail account and saw an email from an unknown subject with a Gmail address stating this person knew who had hacked him and seemed to be offering assistance. He forwarded that email to Google to see if Google could tell him anything about that account. A short time later he received a telephone call from a blocked number. The voice on the other line stated they were in a "Dark Web" chat room and a group of subjects were talking about going after the victim's cryptocurrency accounts. Myles D. does not have any cryptocurrency but works for a company which is involved in cryptocurrency. He was scared and believed he was talking to the hackers, and hung up the phone.

On 10/28/18, Myles D. received an email from Fidelity informing him that three of his mutual fund accounts had been liquidated and were pending wire transfers. He contacted Fidelity and was able to cancel the wire transfers. The suspect(s) had attempted to transfer approximately $300,000 from the victim's Fidelity account.

(V) Angel A.

I spoke with this victim via telephone on 11/1/18, and she related the following. Angel A. is a resident of Los Angeles, California. On 10/16/18, her AT&T cell phone number ([redacted] stopped

working. A short time later she realized she had lost access to her Twitter social media account ([redacted]). The suspect who was in control of [redacted] began sending bomb threats to airlines from her Twitter account along with racist "Tweets" regarding Former President Barack Obama. The victim contacted Twitter and regained access to her account. She is unaware of any other accounts that were compromised.

(V) James M.

I spoke with this victim via telephone on 11/1/18, and he related the following. James M. is a resident of Bronx, New York. On 10/15/18, his AT&T cell phone number ([redacted]) stopped working. He received an email from Instagram that the password was changed for his Instagram username ([redacted] and the email account associated to his [redacted] Instagram account was changed to [redacted]. The suspect attempted to access his Facebook account, but Facebook stopped the attempt. He believes somebody with the Instagram account @gay hacked him because the victim was taunted on his new Instagram Account by that user via Instagram Direct Message for having lost access to [redacted]. The victim was never able to regain access to [redacted], which he had used for business purposes.

(V) Gabrielle K.

I spoke with this victim via telephone on 10/30/18, and she related the following. Gabrielle K. is a resident of San Francisco. On 10/21/18, her AT&T cell phone number ([redacted]) stopped working. She noticed this when she woke up and her had phone no service. She received an email from AOL that her password was changed and a Gmail notification that her Gmail, Evernote and Dropbox passwords had changed. She also received a notice that her Coinbase cryptocurrency account login information had changed. She was able to disable her Coinbase account before any further actions were taken by the suspect. She then went to an AT&T Store to get a new SIM card.

(V) Matthew R.

I spoke with this victim via telephone on 11/2/18, and he related the following. Matthew R. is a resident of the State of Texas. On 10/23/18, his AT&T cell phone number ([redacted]) stopped

working. While he was still connected on Wi-Fi, he received emails that his email account passwords were reset. He was still logged into those accounts while the suspect was simultaneously in control. He saw emails saying other accounts connected to the email were being reset. Those accounts included [redacted] and [redacted] The suspect also attempted to gain access to his Coinbase, HitBTC, Binance and Bittrex cryptocurrency accounts and his blockchain cryptocurrency wallet. The suspects called him twice asking for blackmail payments of $200,000 in Bitcoin to get all his accounts back. One of the suspects sounded young and Asian and the second suspect sounded Eastern European and seemed like he was trying to disguise his voice.

Suspect telephone number [redacted] and identification of (S) Nicholas TRUGLIA

Records provided by AT&T also indicated that the when the suspect's phone was in control of the identified victim accounts, the phone was located in the New York, New York area. In addition, the records indicated that the phone number [redacted] was connected to the suspect IMEI (359239069326461) on 10/5/18, but that this connection was not reported as a fraudulent SIM Swap by the customer. I believe this is indicative of the suspect using a SIM card in his/her possession to test whether the cell phone is functioning properly and connects to the cell carrier's network. I therefore believe the phone number [redacted] belonged to the suspect.

On 10/26/18, the Honorable Maureen Folan, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to the account associated with the telephone number [redacted]. AT&T provided REACT investigators with records that identified the subscriber as "Jeffrey St. Denis" and included the additional information described below.

On 10/29/18, the cryptocurrency exchange Coinbase provided records to investigators which identified an account associated with the phone number [redacted] the number believed to be associated with the suspect. These records indicated this phone number was used to register a Coinbase account in the name of Nicholas TRUGLIA using the social security number [redacted] and the email

address [redacted]. Another name associated with the account was Jeffrey St. Denis, the same name as shown in AT&T subscriber records for the suspect phone number. The records also included copies of documents the subscriber used to identify himself, which included a Connecticut Driver License in the name of Nicholas TRUGLIA with a date of birth of [redacted] and a U.S. passport in the name of Nicholas St. Denis TRUGLIA (note the middle name that matches the name used in AT&T subscriber information from the suspect account) with a date of birth of [redacted]

TRUGLIA's Coinbase account also showed deposits and withdrawals of cryptocurrency occurring between 1/6/16 and 3/24/18, and then no activity after 3/24/18 until 10/27/18. On 10/27/18, mere hours after the theft of the bitcoins described above, as well as approximately 14.3 Ether ("ETH") from (V) Robert R.'s account with the cryptocurrency exchange Binance, a small amount of Ether (approximately .025 ETH) was deposited into TRUGLIA's Coinbase account. Santa Clara County District Attorney Investigator D. Berry received records pertaining to Robert R.'s account from Binance on 10/27/18 that reflected the 14.3 ETH theft from Robert R.'s account, although that stolen ETH was transferred only once to an exterior address, and has not moved from that address as of the writing of this report.

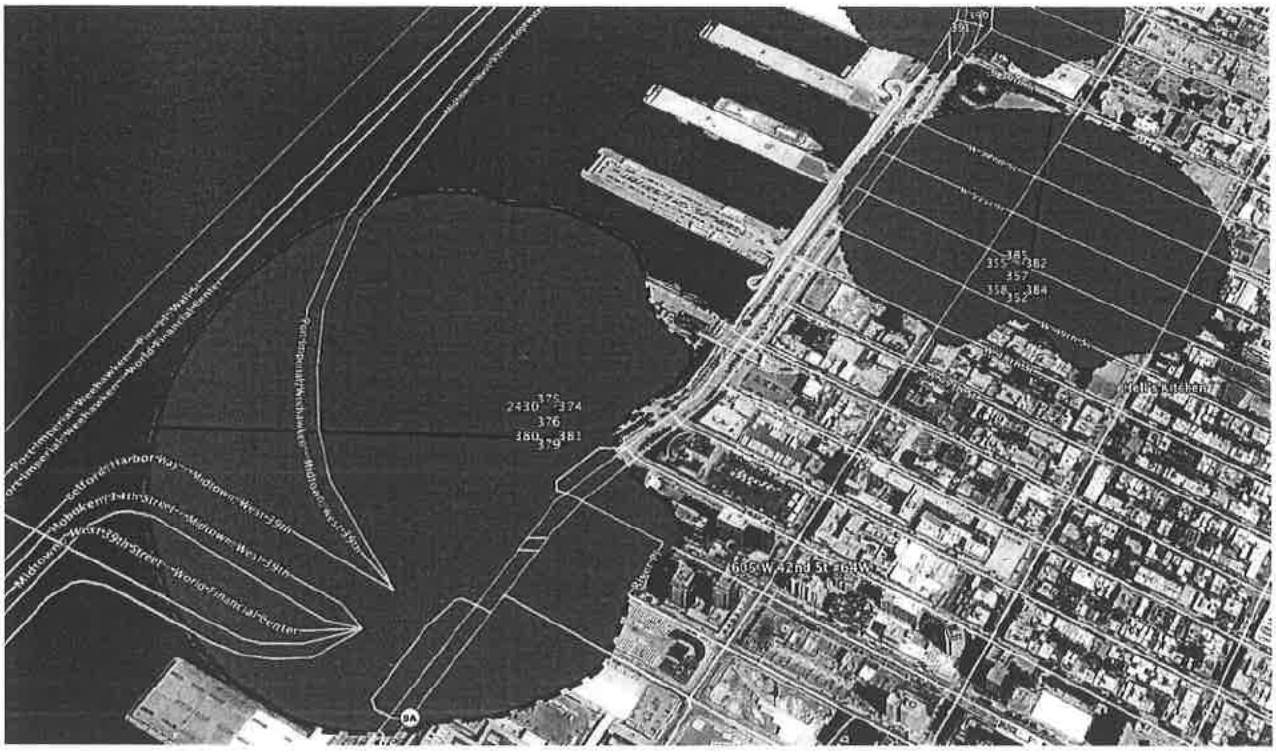
On 11/6/18, REACT investigators received records from the State of New York showing Nicholas TRUGLIA had a New York State Identification Card which listed an address of [redacted], New York 10036.

Sgt. Tarazi examined the records obtained from AT&T and arrived at the following conclusions, in summary (see Sgt. Tarazi's supplemental report for details):

- The records pertaining to TRUGLIA's cell phone account ([redacted]) indicate the owner of the AT&T phone number [redacted] was assigned a SIM card that was physically inserted into an iPhone X with IMEI ending in -5311. Someone removed the SIM card form this iPhone X and placed it inside an iPhone 6 with IMEI ending in -6461, which is the device used to effect the SIM swaps. After approximately 18 minutes, someone removed the SIM

card from the iPhone 6 (-6461) and put it back into the iPhone X (-5311). This SIM card has remained inside the iPhone X (5311) since it was put back in.

- The AT&T cell phone towers to which the iPhone 6 (6461) was connected during the approximate 2 hours and 10 minutes it was in control of victim Matthew R.'s account was consistent with the device having been located at [redacted] NY, as depicted below:



- During that same time period, that same AT&T cell phone tower, as well as several other nearby towers, were used by the iPhone X associated with TRUGLIA's account (5211), as depicted below.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Prior Attempted Account Takeover involving TRUGLIA

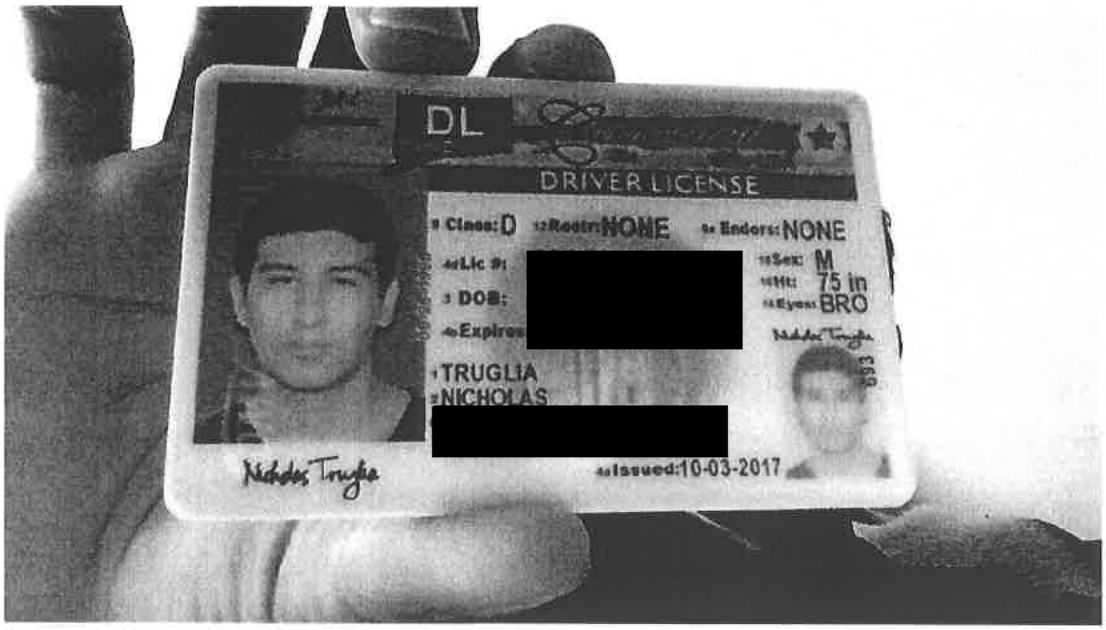
On 10/31/18, Coinbase provided additional information indicating that Truglia has previously been involved in account takeover activity. Coinbase informed REACT investigators that in mid-May 2018, Coinbase received an anonymous tip that someone was going to hack into the Coinbase account of Quinten Capobianco, who had previously died. After Coinbase secured the target account, an external attempt was made to access the account. Coinbase prompted the suspect to provide a photograph of himself holding his ID card as verification, and in response the suspect provided the photograph below.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Based on a comparison to known images, I recognize the person in the photograph above as Nicholas Truglia, who is holding what appears to be a false New York State driver license in Capobianco's name but bearing Truglia's image. Furthermore, Coinbase records indicated that the same device that attempted to access Capobianco's account was then used to log into Truglia's account.

The following three photos were provided as proof of identity for the other Coinbase accounts opened in Truglia's name:

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The following picture is from Truglia's New York Identification, which was obtained through a law enforcement database.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

DMV Photo Request

DMV Photo

Subject Information	
Name:	TRUGLIA,NICHOLAS,S
ClientID:	161405797
Case Number:	108711
DMV Transaction Number:	756281
DMV Transaction Date/Time:	2018-11-05 15:38:31:767

Back

I believe all of the pictures above depict Truglia.

Based on this information, I believe Suspect Truglia attempted to access the deceased person's Coinbase account. This behavior is consistent with the SIM Swapping activity described in this report in the use of impersonation techniques to steal cryptocurrency.

Laundering of stolen funds

Santa Clara County District Attorney Criminal Investigator D. Berry, a REACT Task Force investigator, has examined the flows of cryptocurrency out of Robert R.'s Coinbase, Gemini, and Binance accounts. Investigator Berry observed that the bitcoins transferred out of his Coinbase and Gemini accounts were initially aggregated into a single Bitcoin address, and then moved in a series of transactions that appear intended to obfuscate the source and destination of funds. After some of those layers of movement, proceeds of the theft were deposited into accounts at Binance, a cryptocurrency exchange based in Malta, in a series of transactions apparently structured to avoid account registration requirements (just under 2 bitcoins per transaction, which is the limit above which an account involving "customer due diligence" must be established). Binance provided information related to those transactions, which showed that a series of accounts exhibiting similar behavior had received,

and then promptly withdrawn, the identified stolen bitcoins, which were then aggregated into some overlapping Bitcoin addresses. *See Investigator Berry's supplemental report for additional details.*

Based on my training and experience, I know that moving stolen cryptocurrency through multiple addresses, breaking up stolen amounts into multiple segments of smaller amounts, structuring flows to avoid reporting requirements, and taking steps to avoid meaningful customer due diligence are all consistent with money laundering efforts.

CONCLUSION

Based on the statements of the victims, IMEI number 359239069326461 being connected to S-TRUGLIA's personal cell phone line, Sgt. Tarazi's analysis of phone records, and Investigator Berry's analysis regarding cryptocurrency tracing, I believe S-TRUGLIA committed the following crimes detailed below:

V-Ross:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

487(a) PC – Theft of approximately $500,000 from his Coinbase account

487(a) PC – Theft of approximately $500,000 from his Gemini account

V-Anderson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Twitter account and sending messages

V-Danielson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

502(c)(1) PC and 664/487(a) PC – Unlawfully Accessing Fidelity Mutual Fund and attempting to wire $300,000 from the account

V-Katsnelson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Dropbox account

502(c)(1) PC – Unlawfully Accessing Evernote account

502(c)(1) PC – Unlawfully Accessing Coinbase account

V-Basu:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Yahoo account

664/502(c)(1) PC– Unlawfully Attempting to Access Dropbox account

I am requesting the Santa Clara County District Attorney's Office issue a warrant for the arrest of S-TRUGLIA for the above listed charges.

END REPORT.

PLEO:

TFA C. Tuttle #1945 – Original report
TFA S. Tarazi #2029 – Cell Tower/Geolocation Supplemental Report
TFA D. Berry #47 – Cryptocurrency Tracing Supplemental Report

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

Supplemental Report

Investigation:

On 10-27-2018, REACT detectives received a spreadsheet file from AT&T Fraud Investigator Robert Arno entitled "359239069326461 updated 102718." The first number represents an IMEI number that had been used to conduct SIM swaps. These phone numbers had been identified by AT&T as being used on the above listed IMEI, belonging to an iPhone 6. This IMEI will be referred to by the last 4 digits (6461) throughout the report.

Mobile Number	SIM Card Number	First Use Date
[redacted]	310410704975735	Fri Oct 26 19:50:27 EDT 2018
	310410704975631	Fri Oct 26 17:41:20 EDT 2018
	310410704975737	Wed Oct 24 20:37:24 EDT 2018
	310410704975708	Tue Oct 23 19:44:54 EDT 2018
	310410916138275	Mon Oct 22 23:48:25 EDT 2018
	310410704975736	Sun Oct 21 12:50:23 EDT 2018
	310410704975738	Thu Oct 18 15:37:36 EDT 2018
	310410704975632	Tue Oct 16 14:35:07 EDT 2018
	310410704975633	Mon Oct 15 19:30:26 EDT 2018
	310410704975629	Mon Oct 15 18:31:02 EDT 2018
	310410704975630	Mon Oct 15 15:22:49 EDT 2018
	310410074713285	Fri Oct 05 19:24:43 EDT 2018

Each number above, except for [redacted], was identified by Robert Arno as being an account victimized by an unauthorized SIM Swap by the IMEI ending is 6461. Several of the numbers above have been identified as victims of cryptocurrency theft. See Detective Tuttle's Supplemental Report for further details.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The number [redacted] has been identified as belonging to Suspect Truglia. The phone number had been used to register for a PayPal and Coinbase account in Suspect Truglia's name. See Detective Berry's Supplemental report for further details.

I authored and served a Search Warrant for AT&T records regarding IMEI number ending in 6461 (iPhone 6). I received partial record returns which included the call detail records for the phone number [redacted] and the subscriber information for the rest of the numbers listed above.

Detective Tuttle authored and served a Search Warrant for AT&T records regarding the phone number [redacted] (Suspect Truglia's AT&T phone number).

I examined the call detail records for Suspect Truglia's phone line and I noticed that on 10-5-18 at 23:24:43 (UTC) the IMEI number on the account switched from 354851092905311 (iPhone X) to the iPhone 6 ending in 6461. The records indicate the IMEI switched back to the iPhone 10 (5311) at 23:43:54 (UTC), approximately 18 minutes later. The iPhone X (5311) has been assigned to the Suspect Truglia's account since it switched back.

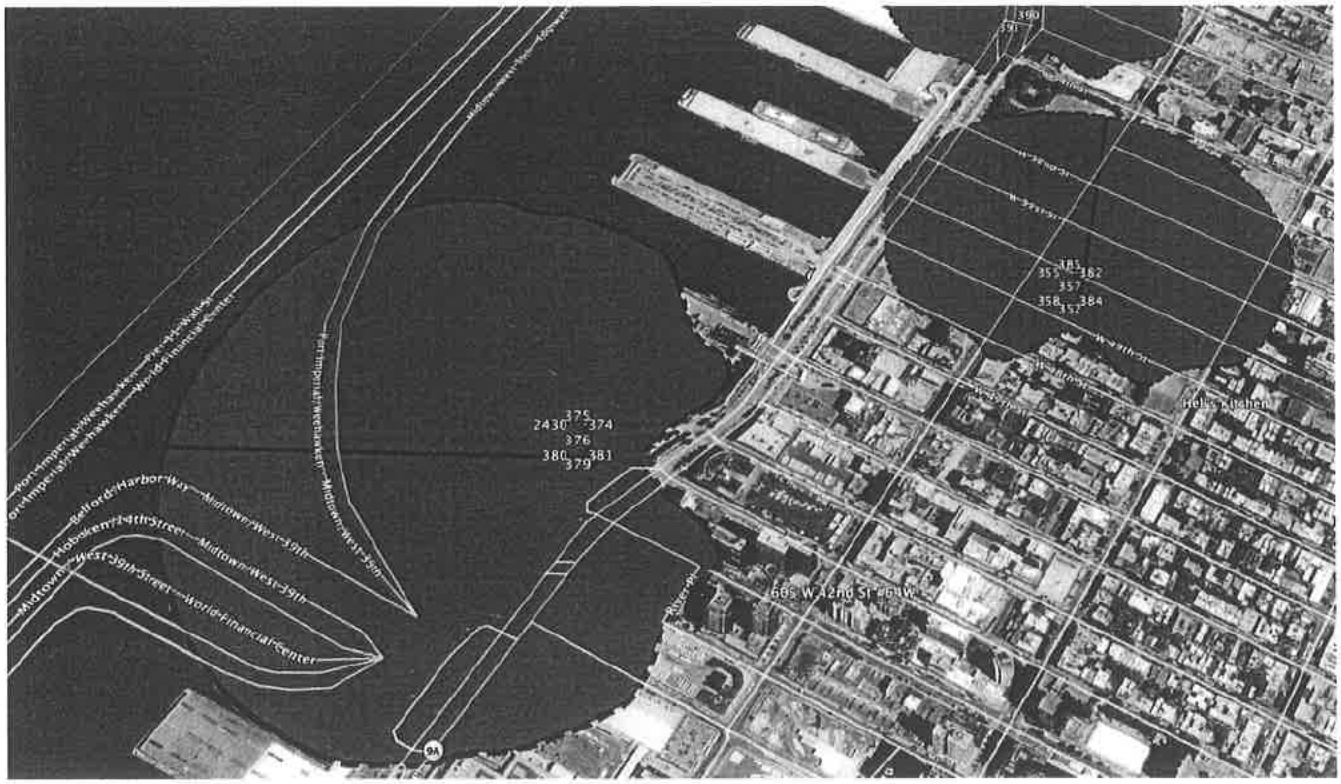
These records mean the owner of the AT&T phone number [redacted] linked to Suspect Truglia was assigned a SIM card that was physically inserted into the iPhone X (5311). Someone removed the SIM card form this iPhone X and placed it inside the iPhone 6 (6461). After approximately 18 minutes, someone removed the SIM card from the iPhone 6 (6461) and put it back into the iPhone X (5311). This SIM card has remained inside the iPhone X (5311) since it was put back in.

I examined the call detail records for the phone number [redacted] and I noticed that 10-23-18 at 22:09:35 (UTC) the IMEI switched from 359407081422499 (iPhone 10) to the iPhone 6 (6461). This IMEI remained active on the account until it switched back to the original IMEI number on 10-25-18 at 01:35:16, approximately 2 hours 25 minutes later. This time span is reasonable to explain the victim losing reception on his/her phone, realizing what happened, contacting AT&T and disconnecting the illegally connected phone from their account.

I examined the geolocation data provided by AT&T for two phone numbers discussed above.

The following pictures depict the AT&T cell phone towers the iPhone 6 (6461) was connected to during the approximate 2 hours and 10 minutes it was in control of the victim's account ([redacted]). The address [redacted] NY is placed for reference as it is listed as Suspect Truglia's residential address on his New York issued Identification Card.

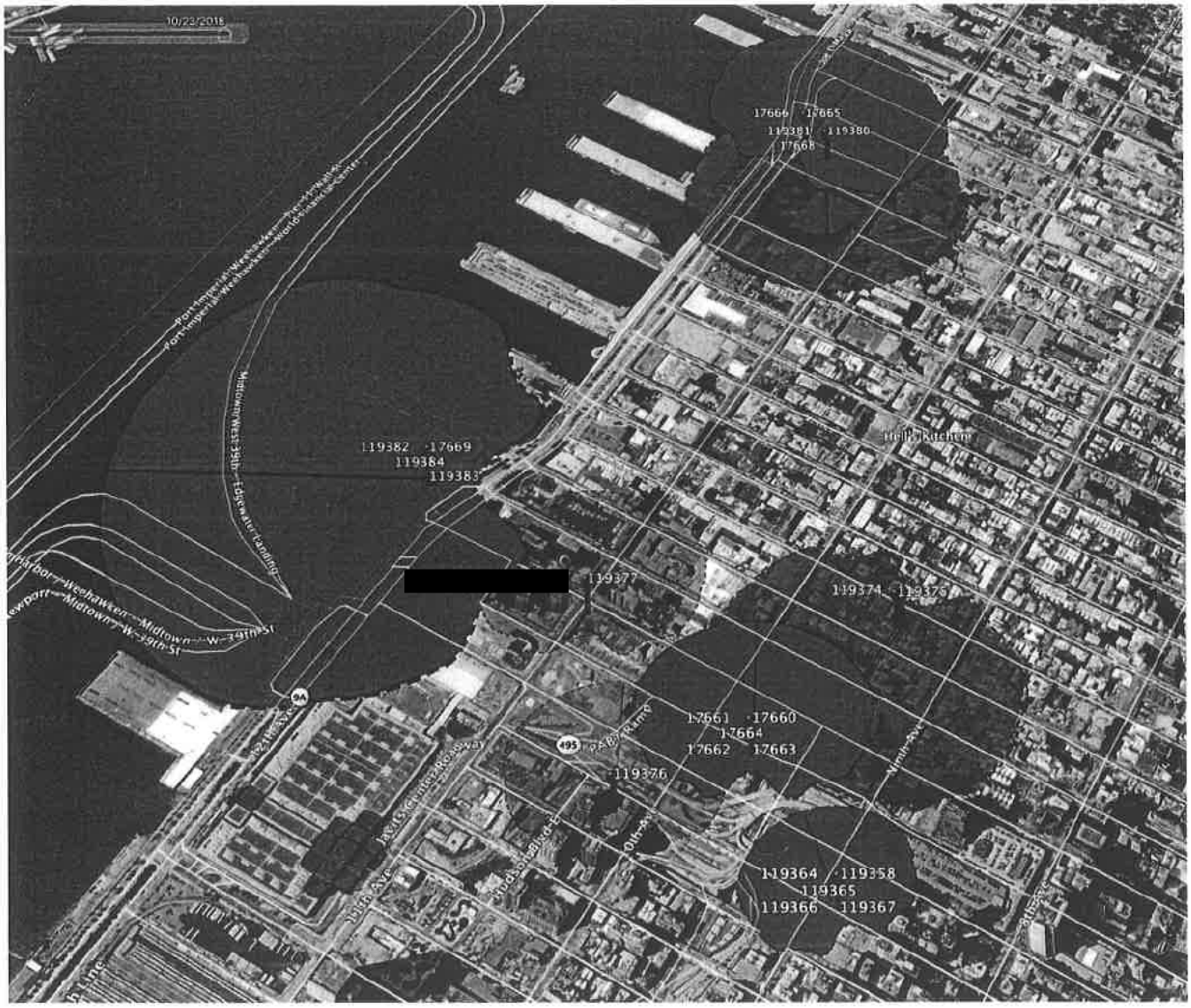
Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The tower to the west of [redacted] is identified by LTE ECGI-ENBID: 28486920-111277.

I further examined the geolocation data for Suspect Truglia's AT&T records for the same time period depicted above (approximately 2 hour 10 minute time window).



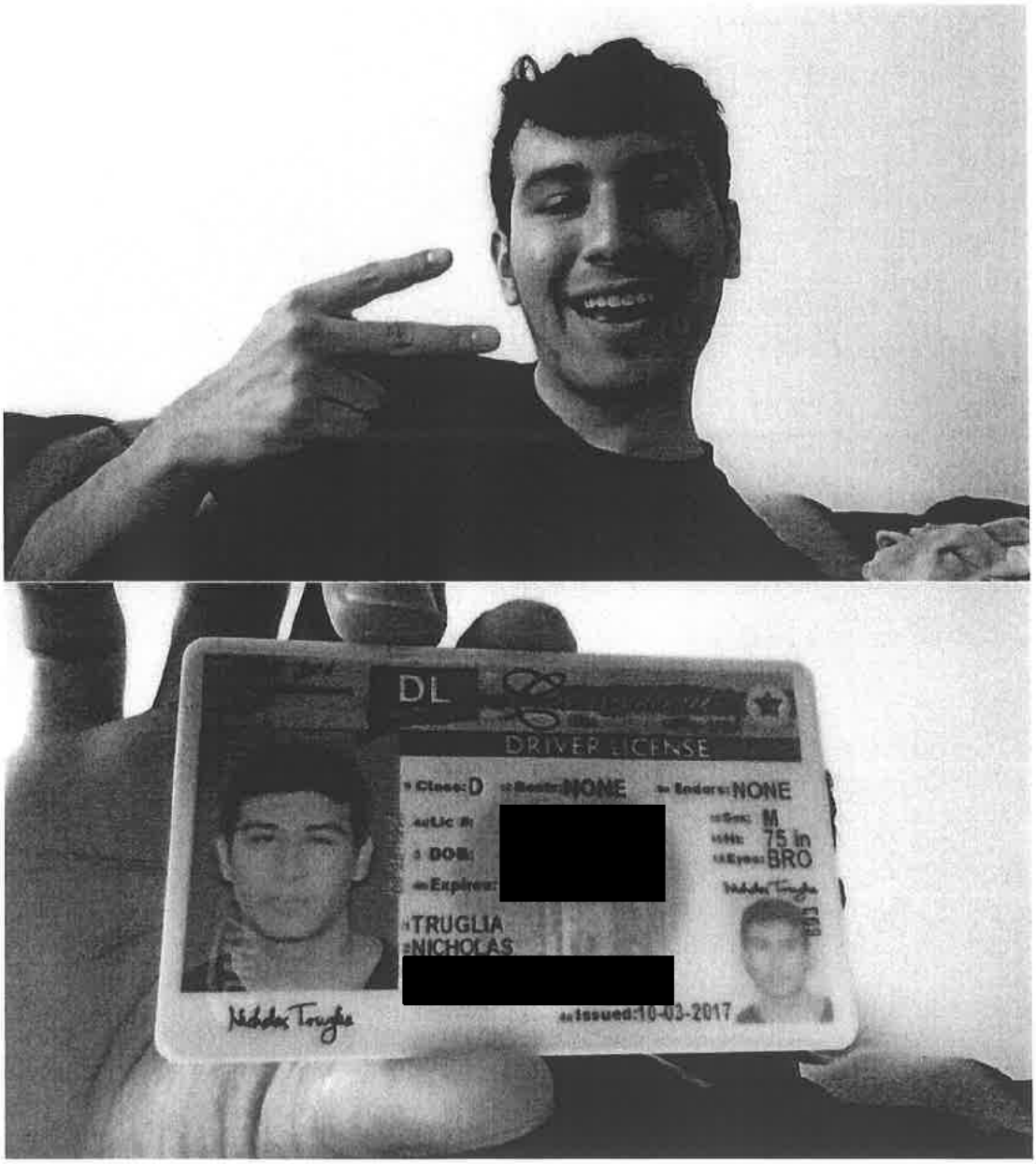
The same AT&T tower LTE ECGI-ENBID: 28486920-111277 was used by Suspect Truglia's AT&T account as well as several nearby towers. This is consistent with both devices being in the same geographical area at the same time.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

On 10-31-18 Coinbase provided additional information indicating that Truglia has previously been involved in account takeover activity. Coinbase informed REACT investigators that in mid-May 2018, Coinbase received an anonymous tip that someone was going to hack into the Coinbase account of Quinten Capobianco, who had previously died. After Coinbase secured the target account, an external attempt was made to access the account. Coinbase prompted the suspect to provide a photograph of himself holding his ID card as verification, and in response the suspect provided the photograph below.

The following three photos were provided as proof of identity on the other Coinbase accounts opened in Suspect Truglia's name:

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE



Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

The following picture is from Suspect Truglia's New York Identification, which was obtained through a law enforcement database.

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

DMV Photo Request

DMV Photo

Subject Information	
Name:	TRUGLIA,NICHOLAS,S
ClientID:	161405797
Case Number:	108711
DMV Transaction Number:	756281
DMV Transaction Date/Time:	2018-11-05 15:38:31:767

Back

I believe all of the pictures depicted above are of Suspect Truglia.

Based on this information, I believe Suspect Truglia attempted to access the deceased person's Coinbase account. This behavior is consistent with the SIM Swapping described in this report as the ultimate goal of the SIM Swapping is to steal cryptocurrency.

Based on the information above, I believe Suspect Truglia to have been in possession of the iPhone 6 (6461) and iPhone X (5311) described above and is responsible for conducting the SIM Swaps listed on page 1 of this report. See Detective Tuttle's Original report for further information.

END REPORT

PLEO:

Sgt. S. Tarazi- 2029